

## APPTIO EU GENERAL DATA PROTECTION REGULATION PROVISIONS

These EU General Data Protection Regulation Provisions (“**GDPR Provisions**”) supplement, are a schedule to and are incorporated into the terms of the services agreement (“**Agreement**”) currently between Apptio, Inc. (“**Apptio**”) and its subscriber/customer (“**Subscriber**”) with regard to Apptio’s Processing of Personal Data on behalf of Subscriber in accordance with the requirements of all laws and regulations of the European Union, the European Economic Area and their member states. These GDPR Provisions will apply to the Processing of Personal Data by Apptio in the course of providing the Apptio software as a service solution (the “**Services**”). These GDPR Provisions do not otherwise disturb or impact any other agreement by and between the parties. The parties agree as follows:

- 1. Process Personal Data as Instructed.** Except to the extent otherwise expressly stated in the Agreement: (i) Subscriber is the controller of Personal Data provided in the context of the Services; (ii) Subscriber hereby appoints Apptio as a Processor to Process such Personal Data; (iii) Apptio shall Process Personal Data as a Processor as necessary to perform its obligations under the Agreement (including any Order thereunder) and otherwise strictly in accordance with the written instructions of Subscriber, except where otherwise required by any applicable law. In the event that Apptio is otherwise required to Process Personal Data by applicable law, Apptio will notify Subscriber without undue delay and the parties will cooperate to ensure that Personal Data is processed to the minimum extent required by applicable law, unless such notification is prohibited by applicable law on important grounds of public interest.
- 2. Confidentiality Restrictions.** Apptio shall ensure that any persons authorised to Process the Personal Data by it (including its employees, contractors, agents and subcontractors) have committed themselves to obligations of confidentiality which are at least commensurate with the confidentiality obligations contained in the Agreement or are under an appropriate statutory obligation of confidentiality; further Apptio shall refer to Subscriber all requests for access to, amendment of, or deletion of Personal Data and any complaints by third parties regarding the handling of such Personal Data.
- 3. Security Measures.** Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Apptio shall implement appropriate technical and organizational security measures which are designed to ensure against (a) unauthorized access to, (b) unauthorized or unlawful alteration, disclosure, destruction or other unauthorized or unlawful Processing of, (c) accidental loss or destruction of, or (d) damage to, the Personal Data. Such technical and organizational security measures shall include as appropriate and without limitation (i) industry standard measures to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services, (ii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident, and (iii) a Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.
- 4. Data Subjects.** Taking into account the nature of the Processing, Apptio shall at all times cooperate with and assist Subscriber in so far as possible to enable Subscriber to meet applicable deadlines and requirements under Applicable Data Protection Laws in relation to a Data Subject’s right (i) of rectification of Personal Data, (ii) of erasure of Personal Data, (iii) to restriction of Processing of Personal Data, (iv) to portability of Personal Data, (v) to object to the lawfulness of the Processing of Personal Data, and (vi) to not be subject to a decision based solely on automated Processing. Apptio shall notify Subscriber, as soon as possible, of any request made by a Data Subject to access Personal Data and shall at all times cooperate with and provide Subscriber with any assistance it may require in order to execute Subscriber’s obligations under Applicable Data Protection Laws.
- 5. Notification of Security Incidents.** In the case of a Personal Data Breach, Apptio shall without undue delay, within 24 hours from Apptio becoming aware of any such incident, notify Subscriber of the Personal Data Breach. To the extent that Apptio has access to such information at the time of the notification, such notification shall (i) describe the nature of the Personal Data Breach, without limitation, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned, (ii) describe the likely consequences of the Personal Data Breach, and (iii) describe the measures proposed to be taken by Apptio to address the Personal Data Breach (provided Apptio will only implement measures such as contacting Data Subjects or notifying the relevant regulator on the instruction of Subscriber), including, where appropriate, measures to mitigate its possible adverse effects. Where, but only to the extent that it is not possible to provide such information at the same time at the notification

of the Personal Data Breach, the information may be provided at a later time but in event as soon as reasonably practicable, and in any event, in sufficient time to enable Subscriber to meet the applicable deadlines under Applicable Data Protection Laws.

6. **Return/Destruction of Personal Data.** In addition to and without prejudice to any obligations set forth in the confidentiality section of these terms or the Agreement, at Subscriber direction and to the extent feasible Apptio shall delete or return all Personal Data to Subscriber at the end of the provision of the applicable Services to which the Processing relates or otherwise upon request, and where and to the extent feasible delete all existing copies held by Apptio (unless applicable law requires the storage of such Personal Data by Apptio) and provide confirmation in writing to Subscriber that it has complied with any such request of Subscriber.
7. **Provide Information as Needed.** Permit Subscriber to take all necessary steps to ensure compliance under Applicable Data Protection Laws, including, but not limited to, making available to the Subscriber all information necessary and allowing for audits and inspections if and to the extent necessary to so comply.
8. **Locations and Consent to Subprocessing.** Apptio shall not subcontract any Processing of Personal Data which Apptio processes as a data processor on behalf of Subscriber as a data controller within the scope of these terms to a third party (“**Subprocessor**”) without Subscriber’s prior consent. Subscriber hereby consents to Apptio engaging (and/or dismissing) subprocessors to Process the Personal Data provided that: (i) Apptio provides notice by posting at <https://www.apptio.com/trust/subprocessors/>; (ii) Apptio additionally provides 30 days prior notice via email notification to any of Subscriber’s personnel who register (free of charge) at the aforementioned web page to receive such notification; (iii) Subscriber may object to the addition of a new Subprocessor appointed by Apptio if Subscriber, in its reasonable discretion, believes that such new Subprocessor in Processing the Personal Data would not comply with these terms, the ADPL, or the Agreement, in which case the parties agree to negotiate in good faith a mutually agreeable alternative. If the objection is valid and no such alternative is agreed within two months of the objection, Subscriber will have the right to terminate, without penalty, any Services for which personal data would be Processed by the new Subprocessor against which the objection was raised; (iv) Apptio shall require by written agreement each Subprocessor’s compliance with the ADPL and will ensure it has the contractual terms in place with such Subprocessor that are required by the ADPL; and, (v) Apptio shall remain responsible for the Subprocessor’s performance under these terms and the Agreement. Apptio will list the locations to which the Personal Data may be transferred in connection with the Service on the aforementioned webpage and shall at all times conduct such transfer in a manner compliant with the ADPL.
9. **Definitions.** For the purposes of this rider:
  - 9.1. “**Personal Data**”, “**Process/Processing**”, “**Controller**”, “**Processor**”, and “**Data Subject**” shall have the same meaning as provided under Applicable Data Protection Laws.
  - 9.2. “**Applicable Data Protection Laws**” or “**ADPL**” means any laws applicable to Apptio or Subscriber in relation to the Processing of Personal Data under this Agreement, including: (i) the legislation and regulations implementing Directive 95/46/EC, (ii) on and with effect from 25 May 2018, the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016) and (iii) any guidance and/or codes of practice issued by the Data Protection Commissioner or other relevant supervisory authority, including the European Data Protection Board.
  - 9.3. “**Personal Data Breach**” shall have the meaning set forth in the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016).